

1. The first step is to identify the key components of the system. This involves understanding the hardware, software, and data involved. For example, in a web application, this might include the server, the database, and the user interface.

2. The second step is to analyze the system's behavior. This involves understanding how the system works and how it interacts with its environment. For example, in a web application, this might involve understanding how the server processes requests and how the database stores data.

3. The third step is to identify the system's vulnerabilities. This involves understanding the system's weaknesses and how they can be exploited. For example, in a web application, this might involve identifying security vulnerabilities in the code or the database.

4. The fourth step is to develop a plan to address the vulnerabilities. This involves determining the steps that need to be taken to fix the vulnerabilities and how to implement those steps. For example, in a web application, this might involve updating the code or the database to address security vulnerabilities.

5. The fifth step is to implement the plan. This involves carrying out the steps that were identified in the previous step. For example, in a web application, this might involve updating the code or the database to address security vulnerabilities.

6. The sixth step is to test the system. This involves verifying that the system is working correctly and that the vulnerabilities have been fixed. For example, in a web application, this might involve testing the code and the database to ensure that they are secure.

7. The seventh step is to monitor the system. This involves keeping an eye on the system to ensure that it is still working correctly and that no new vulnerabilities have appeared. For example, in a web application, this might involve monitoring the server logs and the database to ensure that they are secure.

8. The eighth step is to update the system. This involves keeping the system up to date with the latest software and hardware. For example, in a web application, this might involve updating the code and the database to the latest versions.

9. The ninth step is to document the system. This involves creating a record of the system's components, behavior, and vulnerabilities. For example, in a web application, this might involve creating a document that describes the system's architecture and security.

10. The tenth step is to review the system. This involves evaluating the system's performance and determining if any changes need to be made. For example, in a web application, this might involve reviewing the system's security and performance to determine if any updates are needed.

Julian Mercado

1745

[illegible]

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

[illegible]